SYSTEMS AND METHODS FOR AUTHENTICATING AND PROTECTING THE INTEGRITY OF DATA STREAMS AND OTHER DATA

ABSTRACT OF THE DISCLOSURE

Systems and methods are disclosed for enabling a recipient of a cryptographically-signed electronic communication to verify the authenticity of the communication on-the-fly using a signed chain of check values, the chain being constructed from the original content of the communication, and each check value in the chain being at least partially dependent on the signed root of the chain and a portion of the communication. Fault tolerance can be provided by including error-check values in the communication that enable a decoding device to maintain the chain's security in the face of communication errors. In one embodiment, systems and methods are provided for enabling secure quasi-random access to a content file by constructing a hierarchy of hash values from the file, the hierarchy deriving its security in a manner similar to that used by the above-described chain. The hierarchy culminates with a signed hash that can be used to verify the integrity of other hash values in the hierarchy, and these other hash values can, in turn, be used to efficiently verify the authenticity of arbitrary portions of the content file.

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, D. C. 20005
202-408-4000